SECTION J, ATTACHMENT 5

PERFORMANCE SPECIFICATION 0702

FOR

ENTRY CONTROL EQUIPMENT

FOR THE

INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM-IV (ICIDS-IV)

04 May 2007

TABLE OF CONTENTS

1. **SCOPE.**

1.1 Identification.

This Performance Specification (PS) covers the Entry Control Equipment (ECE) subsystem of the Integrated Commercial Intrusion Detection System (ICIDS).

1.2 Subsystem Description

The ECE subsystem functions as a part of the ICIDS to control individual access to restricted areas. The ECE will deny entry to any individual attempting to enter without the proper credentials. Denied entry alarms are reported to the ICIDS central monitoring location for assessment and response. The subsystem will be capable of interfacing with any standard credential, including but not limited to, the DOD Common Access Card (CAC), commercial "Smart" Cards, and those cards and devices utilizing biometric identifiers. The subsystem shall have the capability to store all access transactions for future retrieval.

1.3 Subsystem Overview

There are two (2) applications of the ECE subsystem.

1) Exterior secure areas.
2) Interior secure areas.

Unless otherwise specified, the requirements pertain to all applications.

2. **APPLICABLE DOCUMENTS**

The following documents of the issue in effect on the date of request for proposal form a part of this description to the extent specified herein. In the event of a conflict between the text of this document and the references cited herein, the text of this specification takes precedence.

2.1 Government Documents.

Homeland Security Presidential Directive (HSPD):

HSPD-12	27 August 2004	Policy for a Common Identification Standard for Federal Employees and Contractors

Other Government Documents:

ICIDS-PS-0700	04 May 2007	Performance Specification (PS) for Command, Control, and Display Subsystem of the Integrated Commercial Intrusion Detection System
SEIWG-012	28 February 1994	Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC)
FIPS PUB 201-1, Change 1	March 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors

2.2 Non-Government Documents.

2.2.1 Underwriters Laboratories (UL) Standards.

UL 294	15 August 2005	Access Control System Units.
UL 639	30 September 2002	Intrusion-Detection Units, 7th Ed.
UL 1076	21 March 2005	Proprietary Burglar Alarm Units and Systems.

2.2.2 National Fire Protection Association (NFPA)

NFPA 101	2006	Life Safety Code

(Application for copies should be addressed to the Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062.)

3. **REQUIREMENTS.**

3.1 Description.

The ECE specified herein is to be used in conjunction with the ICIDS, as defined in ICIDS-PS-0700, to control entry and exit to secure areas and to alert security monitors of attempts at unauthorized entry. The ECE configuration described herein is intended to illustrate functional requirements only and is not intended as a design constraint. Entry control devices installed in a remote secure area are directed by a local controller. The local controllers interface, via the Remote Area Data Collectors (RADCs) and the CCDS, to the network controller/enrollment terminal. The size of this network is determined by the number of secure areas requiring entry control. The security level of each local area is utilized to determine if ECE is required and the type of access credential required.

3.1.2 Major Components:

a. Network Controller/Enrollment Terminal,
b. Printer,
c. Network Controller Backup Power Supply,
d. Local Controller,
e. Local Controller Backup Power Supply,
f. Keypad,
g. Card Reader,
h. Biometric Input Device,
i. Combination Keypad/Card Reader,
j. Card Reader Card,
k. Electric Door Locks (Types 1 through 4),
l. Exit Push Button,
m. Entry Control Equipment/Remote Area Data Collector (RADC) Interface,
n. Badging Station.

Note: Not all sites will require all major components.

3.1.3 UL Listing.

ECE components shall be either UL listed or meet the requirements of UL 294.

3.2 Reliability.

The network controller/enrollment terminal and local controller shall each have a minimum Mean-Time-Between-Failure (MTBF) of 82,000 hours. The entry/exit control devices (keypad, card reader, biometric input device, combination keypad/card reader) shall each have a minimum MTBF of 216,000 hours. The electric door lock, exit push button, and door lock sensor switch shall each have a minimum Mean-Activations-Between-Failure (MABF) of 18,000 activations.

3.3 Construction.

Section 3.2 of ICIDS-PS-0700 shall apply.

3.4 Maintainability.

Section 3.3 of ICIDS-PS-0700 shall apply.

3.4.1 Maintenance Ratio.

Maintenance ratio is defined as the ratio of the total active maintenance man-hours required (scheduled and unscheduled) to the total operating time. Man-hours for repair of replaced components and scheduled before-and-after operation checks are excluded. The maintenance ratio for both the network controller/enrollment terminal and local controller shall not exceed 0.000006. The maintenance ratio for entry/exit control devices (keypad, card reader, biometric input device, combination keypad/card reader) shall not exceed 0.000002. A maintenance schedule shall be established prior to the start of any testing.

3.4.2 Preventive Maintenance.

Section 3.3.4 of ICIDS-PS-0700 shall apply.

3.5 Performance Characteristics.

3.5.1 General System Functions.

When the entry control equipment is installed and operational with the ICIDS console, it shall function as a combined system. The system shall:

a. verify the validity of requests for access and either permit or deny access,

b. notify the requester of acceptance or denial,

c. output the proper control signal to open the access point, lock after access is completed, and provide a door unlocked alarm if the door does not close and lock within the specified time,

d. allow the requester a preprogrammed number of additional requests for access if access is denied on the first request. An access-denied signal shall be output at the entry control device (e.g., red LED at the keypad), at the network controller (e.g., printer and display message), and at the operator console if additional requests for access are denied,

e. allow a duress alarm to be output by the entering of a special code into a keypad or by activating a panic switch. Display the duress alarm at the network controller and operator console, but provide no indication of duress alarm at the local controller or keypad,

f. have a minimum throughput of 6 authorized entries per minute.

3.5.1.1 Major Component Functions.

3.5.1.1.1 Network Controller/Enrollment Terminal.

The network controller/enrollment terminal shall be a programmable device which serves as the ECE network central processor, functions as an enrollment terminal, manages the enrollment database, provides enrollment data to the connected local controllers, and provides an interface either to create a badge or exchange the enrollment data with existing badging systems. The major components of the network controller/enrollment terminal are a display, alphanumeric keyboard, CPU, non-volatile memory, printer, removable storage media, local controller communication port(s), and back-up power supply.

3.5.1.1.2 Network Controller/Enrollment Terminal Functions.

The network controller/enrollment terminal shall:

a. provide enrollment capability. The network controller/enrollment terminal shall provide the hardware and software necessary to enroll and delete users from the system and create badges as needed. As a minimum, enrollment shall specify and allow control of a specific user's access to specified areas, at specified dates and times,

b. provide the following database management functions as a minimum: create a user file or record, append new users to the database, modify data for existing users, and backup all or user selected portions of the enrollment database to removable storage media. The database shall be capable of supporting at least 100,000 individual users having a card, a Personal Identification Number (PIN), a photograph, biometric data, personnel information, other credential, and combinations of credentials. The database shall contain, as a minimum for each enrolled user, the user's name, employee identification, card identification, and PIN. Data specifying identification of personnel shall be protected by passwords level of access,

c. provide a non-volatile storage device for the system software and enrollment database. The system shall have the capability to automatically reinitialize when power is restored after an equipment failure or power outage without loss of the database or necessary operating data,

d. provide for at least four levels of operator access to the functions of the network controller/enrollment terminal. The capability shall be provided to assign the system functions to any of the four operator access levels. Operator access may be controlled by password, card, PIN, or other positive means of identification,

e. provide automatic non-volatile storage of at least the 1,000,000 most recent events (e.g., entry approvals, entry denials, duress alarms, etc.). When this historical log becomes full, new events shall replace the oldest events in a first-in-first-out fashion. The system shall provide the capability to erase, print, and backup all or part of the historical log to make space available for new events. A warning message shall be displayed to the operator when the historical log is nearly full,

f. display all system alarms (e.g., duress, door unlocked, AC power loss, etc.). The display shall be visual, of a type adequate to allow, as a minimum, alphanumeric messages to be reported clearly to the operator,

g. provide a printer and associated software to automatically print events specified by the system maintainer in a format specified by the system maintainer as the events occur (e.g., automatic exception reporting). The printer software shall also provide the capability to generate reports in a format specified by the system maintainer which are keyed to any field of the database (e.g., all events between specified times, for specified users, at specified portals, etc.). Printing reports shall be accomplished on-line and not interfere with normal system operation,

h. provide for control and communications to a minimum of 64 local controllers (expandable in modular increments to full system capacity). The network controller shall be capable of communicating with local controllers separated by a distance of up to sixteen kilometers without repeaters. The sixteen kilometer minimum communication distance shall apply to any communication architecture (i.e., multidrop loop, star (individual), etc.). The use of fiber optics in lieu of hardwired lines is permissible,

i. automatically downloads the appropriate initial database information and appropriate database changes to each local controller to which the specific enrollment information applies,

j. incorporate built-in diagnostics implemented in software/firmware, hardware, or both. Each time the processor is powered it shall automatically execute a series of built-in tests and report equipment malfunctions, configuration errors, and inaccuracies to the printer or display. Diagnostic aids shall be provided within the network processor to aid in set-up, maintenance, and troubleshooting.

3.5.1.1.3 Network Controller/Enrollment Terminal Backup Power Supply.

An Uninterruptible Power Supply (UPS) shall be available, which shall meet the requirements stated in paragraph 3.4.2.1.10 of ICIDS-PS-0700.

3.5.1.1.4 Local Controller.

The local controller shall be capable of complete stand-alone entry control operation after enrollment information is downloaded from the network controller/enrollment terminal.

The local controller also shall:

a. be capable of controlling access (entry and exit) to a minimum of two doors and shall be capable of incremental increases to eight doors,

b. interface to up to eight electric door locks with or without door lock sensors, and sixteen entry/exit devices (i.e., keypads, card readers, biometric devices, or combinations thereof). Note: The sixteen entry/exit devices are divided into eight entry devices and eight exit devices corresponding to the eight doors,

c. be capable of controlling access of not less than 10,000 users, each identified by individually unique cards, PINs, biometric identifiers, or combinations thereof,

d. deny any card, PIN, biometric identifiers, or combination thereof, not authorized for that particular controller,

e. be capable of providing at least four security levels to which each user can be assigned. Any attempt to access an area beyond any individual's pre-defined security level shall result in an access denial alarm after the preprogrammed number of attempts,

f. restrict the time between the access request and allowed access to less than 3 seconds or a longer time, up to 10 seconds, as approved by cognizant authority and selected by the system maintainer. The door lock shall be open to allow access for no longer than the time entered by the system maintainer. A door unlocked alarm shall be transmitted to both the network controller and RADC if any door remains open or otherwise unlocked longer than the 3 second entry time or longer than the entry or exit time selected by the system maintainer,

g. provide the capability for the incorporation of anti-passback functions. Once an authorized individual has passed through a portal, the system shall not allow use of the same identifier to allow entry through any portal of the same security level or lower until the individual has left the area through any portal of the same security level. Any attempt to violate the anti-passback procedures shall result in an entry denial alarm,

h. have an internal battery to prevent loss of volatile memory in the case of power failure,

i. incorporate continuous line supervision of at least communications and power status,

j. provide the database management functions necessary for the local controller database,

k. provide a memory buffer which shall be updated as required to contain the most recent 1,000 events (minimum) in a first-in-first-out fashion. In the event of a communication loss or interruption, the local controller shall upload this buffer to the network controller once communication is restored,

l. provide communications to the network controller, or other local controllers depending on system architecture. The local controller shall be capable of communicating to the network controller, either directly or via other local controllers, separated by a distance of up to sixteen kilometers without repeaters. The sixteen kilometer minimum communication distance shall apply to any communication architecture (i.e., multidrop loop to other local controllers, star (individual) directly to the network controller, etc.). The local controller shall communicate all events (access approved, denied, tamper, duress, etc.) to the network controller as they occur. The communication links shall be such that the use of fiber optics is permissible,

m. provide keypad and card reader line supervision. Line supervision shall be provided whether the keypad is interfaced directly to the local controller or to the card reader such that any opening or shorting shall result in a tamper alarm transmitted to the network controller and to the RADC,

n. be provided with a tamper switch(s) for each enclosure housing) opening, local controller, keypad, or card reader. Opening or attempted removal of an enclosure (housing), or enclosure (housing) cover will result in declaration of a tamper alarm.

3.5.1.1.5 Local Controller Backup Power Supply.

Backup power supply shall meet the following requirements:

a. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

   (1) 120/208/240 Vac, 60 Hz.
   (2) 220 Vac, 50 Hz.

b. Include battery backup capable of supplying sufficient power to the local controller during facility power interruptions, for a minimum of 8 hours, at the lowest specified temperature,

c. The battery shall be sufficiently recharged, within 12 hours after the return of primary power, to provide power through another minimum 8 hour primary power interruption,

d. Continuously monitor the battery voltage. If an over-voltage condition is measured at the battery terminals, the primary AC supply and battery charging circuit shall be disabled and operation shall continue on the battery. If an under-voltage condition is measured at the battery terminals while operating from the battery, the positive battery lead shall be disconnected to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output out-of-tolerance condition is measured, indicating a power supply failure, both the primary AC and battery shall be disabled. Any power loss shall be reported to the PMC,

e. Be capable of sustaining momentary overloads of 125% of rated capacity for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds,

f. Include EMI, transient, and surge protection in accordance with ICIDS-PS-600, paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbance, or to localize damage to easily repairable, low-cost components.

3.5.1.1.6 Keypad.

The keypad may be used alone or in conjunction with a card reader to control access or exit through a locked door by means of a unique combination of alphanumeric keys entered by a user.

3.5.1.1.6.1 Keypad Functions.

As a minimum, the keypad shall:

a. provide a minimum of ten alphanumeric character keys,

b. read the sequence of keys entered by the user, the user's (PIN), and communicate the sequence to the local controller,

c. provide no restriction to the length of the key sequence (PIN) up to a limit of ten characters (i.e., the length of the PIN may be variable for each installation site),

d. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green LED for entry approved) in response to a signal from the local controller.

3.5.1.1.6.2 Keypad Power.

Keypad power may be supplied by the local controller, card reader, or other source as necessary.

3.5.1.1.6.3 Keypad Physical Characteristics.

The keypad, if used as the sole entry controller, shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with a card reader, the keypad may be in the same enclosure with the reader. In either case, the enclosure shall be tamper protected.

3.5.1.1.7 Card Reader.

The card reader shall operate using any one or more of the ID card technologies identified in FIPS PUB 201-1 Change Notice 1 and HSPD-12.

3.5.1.1.7.1 Card Reader Major Functions.

As a minimum, the card reader shall:

a. read encoded cards and communicate the card information to the local controller,

b. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green LED for entry approved) in response to a signal from the local controller.

3.5.1.1.7.2 Card Reader Power.

Card reader power may be supplied by the local controller or other source, as necessary.

3.5.1.1.7.3 Card Reader Physical Characteristics.

The card reader, if not used in conjunction with a keypad, shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with a keypad, the card reader may be in the same enclosure with the keypad. In either case, the enclosure shall be tamper protected.

3.5.1.1.8 Biometric Input Device.

The biometric input device may be used alone or in conjunction with a card reader or other devices, as necessary, to control access to a secure area by means of a set of biometric identifiers. It operates by sensing the physical characteristics presented (finger tip, palm, etc.) and converting them to digital parameters used for identification.

3.5.1.1.8.1 Biometric Input Device Major Functions.

As a minimum, the biometric input device shall:

a. sense the physical characteristics presented (finger print, hand geometry, iris, etc.), convert them to the digital parameters used for identification, and communicate the parameters to the identification database,

b. provide an indication of entry/exit authorized or unauthorized (e.g., red LED for entry denied, green LED for entry approved), if operating as a stand alone device.

3.5.1.1.8.2 Biometric Input Device Power.

Biometric input device power may be supplied by the local controller or other source as necessary.

3.5.1.1.8.3 Biometric Input Device.

The biometric input device shall be provided in its own enclosure, suitable for flush and surface mounting. If used in conjunction with another device, the biometric input device may be in the same enclosure with the other device. In either case, the enclosure shall be tamper protected.

3.5.1.1.9 Combination Keypad/Card Reader.

The combination keypad/card reader shall provide the combined functionality of the individual keypad and individual card reader specified in 3.7.1.1.6 and 3.7.1.1.7, respectively. Either, or both, may be utilized with the biometric input device specified in 3.7.1.1.8, as necessary.

3.5.1.1.10 Card Reader Cards.

Card reader cards shall:

a. be compatible with the card reader specified in 3.7.1.1.7 and 3.7.1.1.8.

b. be not less than 5.08 cm by 7.62 cm or greater than 6.35 cm by 8.89 cm in size,

c. be resistant to forgery, tampering, alteration, and unauthorized extraction of data,

d. be provided with unique identifier codes. A minimum of 10,000 identifier codes shall be available,

e. be designed to last not less than 2 years,

f. be compliant with the requirements of FIPS 201-1 and HSPD-12.

3.5.1.1.11 Electric Door Locks.

Electrical door locks shall be of the electrical release type and shall interface to the local controller and be fully compatible with the rest of the entry control equipment of this Performance Specification. They shall be reversible for use on left-hinged and right-hinged doors. The electric door locks shall be provided with sensors to detect if the locking mechanism is locked or unlocked. These sensors shall be so designed that they detect the actual condition of the locking mechanism. The electric door locks shall be available both with and without the sensors.

3.5.1.1.11.1 Electric Door Lock Safety.

Electrical door locks shall meet the life safety requirements of NFPA 101, Life Safety Code 2006.

3.5.1.1.12 Electric Door Lock Power.

The electric door locks may be powered from the local controller, keypad, card reader, combination keypad/card reader, or other source as necessary.

3.5.1.1.13 Master Key.

All electric door locks shall have a provision for manual mechanical override using a master key.

3.5.1.1.14 Exit Push Button.

An exit push button shall be available for installation in the protected area by a door controlled by entry control equipment when anti-passback procedures are not required. The exit button, when pressed, shall release the electrical door lock for a preset time adjustable for between 2 and 10 seconds.

3.5.1.1.15 Emergency Egress.

An emergency egress capability shall be available to release the door lock and provide an alarm to the network controller of an emergency override.

3.5.2 Interface.

3.5.2.1 Keypad Interface.

The keypad shall interface with the local controller either directly or via a card reader when used in conjunction with a card reader. The interface shall communicate the user's PIN to the local controller and shall communicate the entry/exit authorized/unauthorized signal from the local controller.

3.5.2.2 Card Reader Interface.

The card reader shall interface with the local controller. The interface shall communicate the user's card information and keypad PIN, when used in conjunction with the keypad, to the local controller and shall communicate the entry/exit authorized/unauthorized signal from the local controller.

3.5.2.3 Biometric Input Interface.

The biometric input device shall interface with the local controller either directly, when operating in a stand alone mode, or through a card reader or other device as necessary. The local controller shall communicate the entry/exit authorized/denied signal for display.

3.5.2.4 ECE System/RADC Interface.

Section 3.4.2.2.8 of ICIDS-PS-0700 shall apply with the following additions.

3.5.2.4.1 Physical Interface.

The field wiring and internal wiring shall meet the conditions specified in UL 294, sections 10 through 17.

3.5.2.4.2 Electrical Interface Outputs.

All output signals shall last for 350 ± 100 milliseconds. The outputs shall have form "C" contacts rated at 0.25 A at 24 Vdc.

3.5.2.5 Enrollment/Badging Station.

Station shall include:

a. RSM Workstation with computer, keyboard and mouse or trackball device
b. Color Monitor
c. PC Camera
d. ID Card/Token Printer
e. Report/Logging Printer
f. Uninterruptible Power Supply (UPS)
g. DoD Common Access Card (CAC) Reader

3.5.3 Enclosures.

3.5.3.1 Construction.

All enclosures of entry control equipment shall meet UL 294, section 7.

3.5.4 Detection/False-Alarm Performance.

3.5.4.1 Access-Authorized Error Rate.

The rate at which the entry control equipment, when configured in its maximum configuration, denies access to an authorized, enrolled individual shall be less than 1.0 percent.

3.5.4.2 Access-Denied Error Rate.

The rate at which the entry control equipment, when configured in its maximum configuration, allows access to an unauthorized individual shall be less than 0.01 percent.

3.6 Human Factors Engineering (HFE).

Section 3.8 of ICIDS-PS-0700 shall apply.

3.7 Safety.

Paragraph 3.9 of ICIDS-PS-0700 shall apply.

3.8 Environmental Requirements.

3.8.1 Natural Environment.

Section 3.10.1 of ICIDS-PS-0700 shall apply.

3.8.1.1 Interior Components.

3.8.1.1.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -30 C and +60 C.

3.8.1.1.2 Operating Conditions.

a) Temperature. The ECE components shall be able to operate, as specified herein, in any temperature between +10C and +40C.

b) Relative Humidity. The ECE components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

3.8.1.2 Exterior Components.

3.8.1.2.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -30C and +50C.

3.8.1.2.2 Operating Conditions.

a. Temperature. The ECE components shall be able to operate, as specified herein, in any temperature between -10C and +50C.

b. Relative Humidity. The ECE components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

c. Rain. The ECE exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 57.

d. Dust. The ECE exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour, as specified in UL 639, Section 58.

3.8.2 Impact Conditions.

The ECE components shall not be damaged and shall operate, as specified herein, when subjected to the jarring test as specified in UL 1076 Section 39.

3.8.3 Vibration Conditions.

The ECE Shall not be damaged by vibration when also tested as specified in UL 639, Section 37.

3.9 Electromagnetic Compatibility.

3.9.1 Electromagnetic Radiation.

The ECE components shall comply with the requirements of Federal Communication Commission (FCC) Standard Part 15, Class B equipment.

3.9.2 Induced Environment.

The ECE components shall meet lightning, EMI transient, and power surge requirements of UL 1076, Sections 44 and 45.

3.9.3 Lightning.

Equipment shall be protected to prevent equipment damage as a result of transients conducted into the equipment through power, communication, and/or control lines by natural phenomena, such as lightning, or to localize damage in easily repairable, low-cost components.

3.10 Finish.

Unless otherwise specified, the portions of the components subject to corrosion shall be cleaned, treated and painted.

3.11 Identification Plate or P/N Marking.

All components of the ECE shall be identified with make, model/part number and serial number in accordance with UL 1076.

3.12 Workmanship.

The workmanship shall be in accordance with best commercial standards and practices. These requirements are applicable to wiring, welding, brazing, plating, riveting, finishes, machine operations, screw assemblies, and freedom of parts from burrs, sharp edges, or any other damage or defect that could make the part (or equipment) unsuitable for the purpose intended.

4. **VERIFICATION**

Verification is the process of inspection to show that the ECE system, while functioning within the ICIDS, meets the requirements of this specification. All inspection results shall be documented in contractor prepared reports. The Government reserves the right to perform any of the inspections set forth in this specification, where such inspections are deemed necessary to ensure supplies and services conform to the prescribed requirements.

4.1 Methods of Verification.

Methods utilized to accomplish verification are as defined in Paragraph 4.1 of ICIDS-PS-0700, using Table 1 of this specification.

4.2 Performance Verification Test (PVT)

4.2.1 Performance Verification Test – 1

Performance Verification Test – 1 shall be as stated in ICIDS-PS-0700, paragraph 4.2.1, utilizing Table 1 of this specification.

4.2.2 Installed Performance Verification Test – 2

Installed Performance Verification Test – 2 shall be as stated in ICIDS-PS-0700, paragraph 4.2.2, utilizing Table 1 of this specification.

4.2.3 Installed System Acceptance Test

Installed System Acceptance Test includes analysis, examination, and System Acceptance Test (SAT) of each installed ICIDS-IV system, subsequent to the first system, to verify performance prior to

Government acceptance. Contractor generated, Government approved test plans and procedures shall be utilized using the test methods described in Table 1 to verify acceptable system performance.

Table 1: Methods to Accomplish Verification

Paragraph	C/A	C/E	C/T
3.5.1 General System Functions			x
3.5.1.1.1 Network/Enrollment Terminal		x	
3.5.1.1.2 Network/Enrollment Functions			x
3.5.1.1.3 Net/Enroll Backup Power			x
3.5.1.1.4 Local Controller		x	
3.5.1.1.5 Local Controller Backup Power			x
3.5.1.1.6.1 Keypad Functions			x
3.5.1.1.7.1 Card Reader Functions			x
3.5.1.1.8.1 Biometric input device Functions			x
3.5.1.1.9 Combined/Keypad/Card Reader			x
3.5.1.1.10 Card Reader Cards		x	
3.5.1.1.11 Electric Door Locks		x	
3.5.1.1.14 Exit Push Button			x
3.5.2.1 Keypad Interface			x
3.5.2.2 Card Reader Interface			x
3.5.2.3 Biometric Input Interface			x
3.5.2.4 ECE/RADC Interface			x
3.5.4 Detection/False Alarm Performance	x		x
3.6 HFE.		x	
3.7 Safety.		x	
3.8.1.1.1 Non-operating conditions.	x		
3.8.1.1.2 Operating conditions.	x		
3.8.2 Impact.	x		

Paragraph		C/A	C/E	C/T
3.8.3	Vibration.	x		
3.9.1	EMI radiation.	x		
3.9.2	Induced environment.	x		
3.10	Finish.		x	
3.11	ID Plate or P/N Marking.		x	
3.12	Workmanship.		x	

5. **PACKAGING**

Packing requirements will be specified in Section D of the contract.

6. **NOTES**

6.1 Intended Use.

The ECE covered by this Performance Specification is intended to be a subsystem of the ICIDS which is for fixed, ground-based installation use.

6.2 Definitions.

Definitions of terms as used in this specification.

6.2.1 Damage.

Damage is defined as deformation, corrosion, loosening of parts, breakage, change of fit of any part, physical change which impairs the mechanical integrity of the component, evidence of delamination or water penetration into integrated circuits, printed circuit boards or parts resulting in non-conformance of a component to the provisions of this Performance Specification.

6.2.2 “Smart Card”

A “Smart Card” is defined as an identification credential that contains special information of an individual nature such as digital certificates, digital signatures, and/or biometric identifiers.

6.2.3 Biometric Identifier

A Biometric identifier is a set of biological characteristics that are unique to an individual and may be used to positively identify a person. Examples of biometric identifiers are fingerprints, facial characteristics, iris pattern, and hand geometry.

6.2.4 Biometric Input Device

The biometric input device is defined as the input device which senses the biometric parameters being used as an identifier. Examples are a fingerprint pad, an iris scanner, a hand geometry sensing plate, and other biometric sensors. The input sensor shall have processing circuits and associated electronics included within its enclosure and transmit sensor data to the database or local controller. It shall operate in conjunction with other devices such as a card reader or keypad and communicate with a remotely located database.